Windows XP

Unit P

Administering Your Computer

Objectives

- Explore Windows administrative tools
- Monitor activity with Event Viewer
- Manage an event log
- Create a performance chart
- Set up an alert
- View Computer Management tools
- Understand disk file systems
- Manage disks
- Monitor local security settings

If you have purchased a computer and set it up in your home, you are that computer's administrator. Computers on a network in an institution, such as at a university, are called clients. The clients are managed by one or more system or network administrators, who have the task of ensuring that the network and its services are reliable, fast, and secure. Although most network administration takes place on the server end, clients must also be administered. Windows XP includes administrative tools that make it easy to ensure that client computers are operating as they should. John Casey, owner of Wired Coffee Company, is considering setting up a few computers for patrons to use while relaxing at Wired Coffee. He wants to understand more about how those computers would need to be administrated and secured. He asks his system administrator, Margaret Kolbe, to assist him in understanding Windows XP administrative tools.

Unit P

Windows XP

Exploring Windows Administrative Tools

Windows XP offers a set of administrative tools that help you administer your computer and ensure it operates smoothly. The Administrative Tools window, opened from the Control Panel, provides tools that allow you to configure administrative settings for local and remote computers as shown in Table P-1. If you are working on a shared or network computer, you might need to be logged on as a computer administrator or as a member of the Administrators group in order to view or modify some properties or perform some tasks with the administrative tools. You can open User Accounts in the Control Panel to check which account is currently in use or check with your system administrator to determine whether you have the necessary access privileges. Margaret explains that many Windows XP users won't ever have to open the Administrative Tools window, but that computers open to the public or on a network will probably require more maintenance. She suggests, therefore, that John open this window to see the tools available to him.

Steps 1 2 3 4

STOP *If you are working on a shared or network computer, you might not be able to work through all the steps in this unit; however, you can read the lessons without completing the steps to learn what is possible as a system administrator.*

1. Click the **Start button** on the taskbar
   Make a note of the name that appears at the top of the Start menu, which identifies the account currently logged onto your computer.
2. Click **Control Panel**, then click **Switch to Classic View** if necessary
   The Control Panel window opens, displaying the available administrative tools.
3. Double-click the **User Accounts icon**
   The User Accounts window opens, displaying a list of user accounts at the bottom of the window. If the name at the top of the Start menu matches the name associated with the computer administrator account, you have the access privileges to use all the administrative tools.
4. Click the **Close button** in the User Accounts window
   The Control Panel window appears.
5. Double-click the **Administrative Tools icon**
   Figure P-1 shows the tools available on John's computer. Your Administrative Tools window might show other tools or fewer tools if your network administrator has installed additional administrative tools or removed tools.

Trouble?

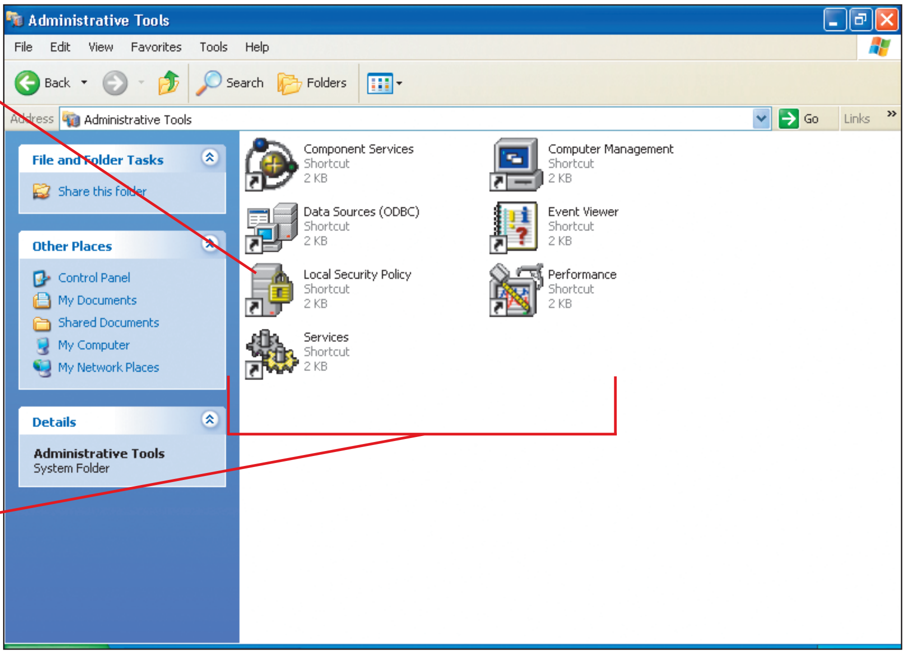
If you are not logged on as a computer administrator, check with your instructor or network administrator to determine whether you need to log off and log on as a Computer administrator.

CLUES TO USE

Accessing administrative tools from the Start menu

If you frequently use the Windows administrative tools, you can save time by adding a menu item to the Start menu, so you can bypass the Control Panel. To add the Administrative Tools menu item to the Start menu and the All Programs menu, right-click the Start button, then click Properties. In the Taskbar and Start Menu Properties dialog box, click the Start Menu tab if necessary, click Customize, click the Advanced tab in the Customize Start Menu dialog box, scroll to the bottom of the Start menu items list, click the Display on the All Programs menu and the Start menu option button under System Administrative Tools, then click OK twice. To access the Administrative Tools menu item, click the Start button on the taskbar. The Administrative Tools menu appears in the right column of the Start menu under the Control Panel menu item and includes a submenu of administrative tools.

FIGURE P-1: Viewing the Administrative Tools window


Administrative Tools
File Edit View Favorites Tools Help
Back
Search
Folders
Address Administrative Tools
Go
Links
File and Folder Tasks
Share this folder
Other Places
Control Panel
My Documents
Shared Documents
My Computer
My Network Places
Details
Administrative Tools
System Folder
Component Services Shortcut 2 KB
Computer Management Shortcut 2 KB
Data Sources (ODBC) Shortcut 2 KB
Event Viewer Shortcut 2 KB
Local Security Policy Shortcut 2 KB
Performance Shortcut 2 KB
Services Shortcut 2 KB

Available only in the Professional edition

Your list of administrative tools might differ

TABLE P-1: Administrative tools

icon	tool	description
	Component Services	Configures and manages system and application components
	Computer Management	Provides access to administrative tools to manage local and remote computers
	Data Sources (ODBC)	Enables programs to access, trace, and manage data in database management systems
	Event Viewer	Displays monitoring and troubleshooting messages from the system and other programs
	Local Security Policy	Modifies local security policy, such as user rights and audit policies; available only in the Professional edition
	Performance	Displays graphs of system processes and configures data logs and alerts
	Services	Displays, starts, and stops services provided to users by your computer

CLUES TO USE

Network security

A network's security is measured by the degree to which data and resources on the computer are protected from system failure or unauthorized intrusion. One way a network administrator ensures security is by assigning rights to individual users or groups of users. For instance, a user on a client computer running Windows XP that has physical access to a network cannot access network files or resources until the administrator has granted rights to that computer and user. The ability to access administrative tools is assigned only to certain user groups, such as the Administrators group, to protect the unauthorized or accidental modification of important information. If you are a user, or member, in a group that does not have the right to use administrative tools, you might not be able to perform all the steps in this unit or even see some of the tools in Figure P-1. To check membership in a group (available in Windows XP Professional only), double-click the Computer Management icon in the Administrative Tools window, click the Expand indicator next to Local Users and Groups in the left pane, click the Groups folder, then double-click a group icon in the right pane to display a list of members in the Properties dialog box. To add members, click Add in the Properties dialog box, in the Select Users dialog box type the new member name or select one as indicated, then click OK twice.

Monitoring Activity with Event Viewer

Every time you start Windows, an event-logging service notes any unusual event that occurs, such as a failed logon, the installation of a new driver for a hardware device, the failure of a device or service to start, or a network interruption. For some critical events, such as when your disk is full, a warning message appears on your screen. Most events, however, don't require immediate attention, so Windows logs them in an event log file that you can view using the Event Viewer tool. Event Viewer maintains three logs: System, for events logged by Windows operating system components; Security, for security and audit events (such as who logged on); and Application, for program events. When you are troubleshooting problems on your computer, you can use the Event Viewer logs to monitor what activity took place. Margaret asks John to open Event Viewer to see what types of activities have been logged on the computer.

Steps 1234

1. In the Administrative Tools window, double-click the **Event Viewer icon**
   The Event Viewer window opens. The left pane of the window displays the three types of logs maintained by your computer. From the Action menu, you can run commands to save a log to a file or open additional log files, for example, from other computers on the network.

QuickTip

Once you have selected a log from the left pane, click View on the menu bar to open a menu of viewing options, including the option of choosing which columns to display or the order in which they appear.

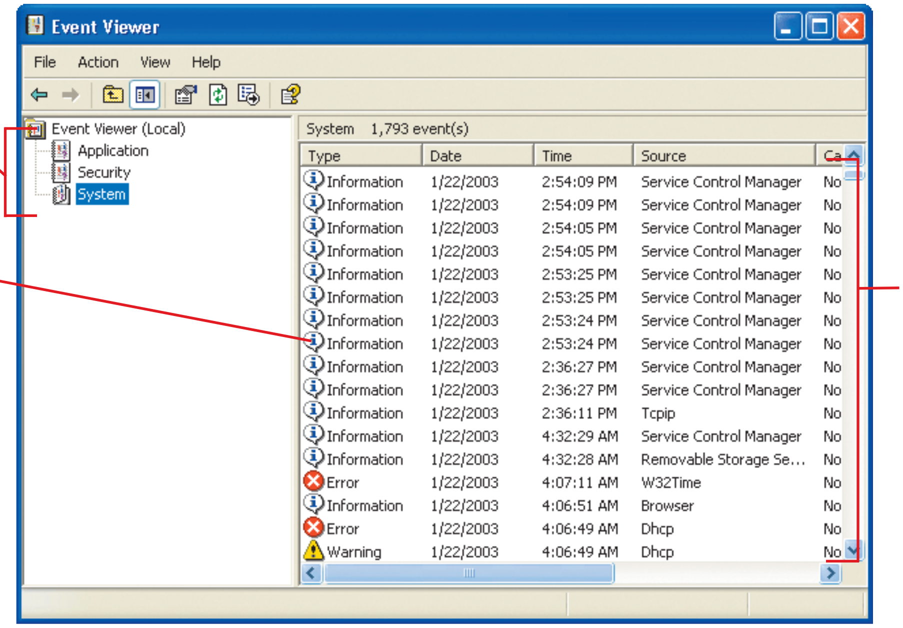
2. In the left pane, click **System** if necessary
   The log for System events appears in the right pane of the Event Viewer window. Figure P-2 shows the System window for John's computer. Your log will show different events. You can click any column header to resort the list; by default, items are sorted by date, with the most recent events listed first. The first column, Type, identifies the nature or severity of the event: ℹ indicates a normal event; ⚠ warns that the event might indicate a problem; and ⊗ indicates a more serious error that resulted in the loss of a function or data. See Table P-2 for a description of each column.
3. Double-click an **event** in the right pane
   The Event Properties window for the event you double-clicked opens, showing details of the event. Figure P-3 shows the Event Properties window for a system time error. Additionally, a description appears, and in some cases, a data section at the bottom of the window. Some events generate **binary data** that experienced computer technicians can evaluate to better interpret the event.
4. Click either the **up arrow button** ↑ or the **down arrow button** ↓
   Another event description appears in the window.
5. Click **OK** to close the Event Properties window

QuickTip

If your Security log is blank, then you are not on a network, you don't have the rights to view this log, or there have been no security breaches. Skip Step 6.

6. Click **Security** in the left pane
   If your computer has experienced any security events, such as a user trying to log on using an incorrect password, those events will be listed in the right pane.
7. Click **Application** in the left pane
   The right pane lists all of the events associated with the operation of the various applications on your system. This could include the installation of new programs or errors that have caused your programs to fail.
8. Click **System** in the left pane to return to the System log

FIGURE P-2: System Event log



System 1,793 event(s)

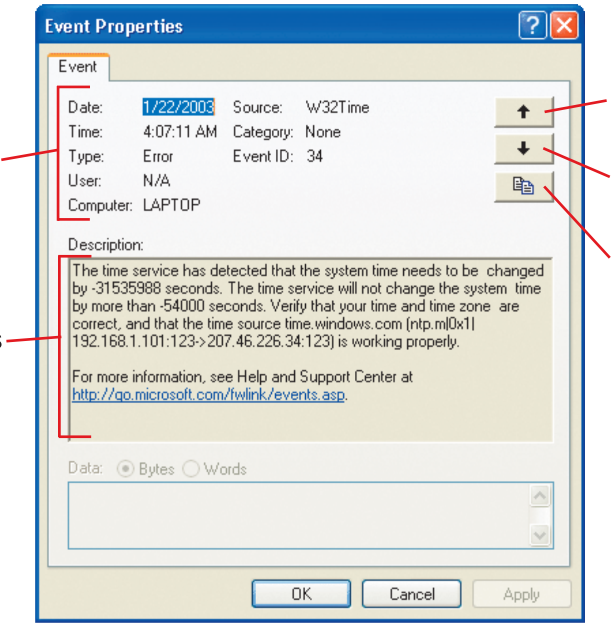
Type	Date	Time	Source	Ca
Information	1/22/2003	2:54:09 PM	Service Control Manager	No
Information	1/22/2003	2:54:09 PM	Service Control Manager	No
Information	1/22/2003	2:54:05 PM	Service Control Manager	No
Information	1/22/2003	2:54:05 PM	Service Control Manager	No
Information	1/22/2003	2:53:25 PM	Service Control Manager	No
Information	1/22/2003	2:53:25 PM	Service Control Manager	No
Information	1/22/2003	2:53:24 PM	Service Control Manager	No
Information	1/22/2003	2:53:24 PM	Service Control Manager	No
Information	1/22/2003	2:36:27 PM	Service Control Manager	No
Information	1/22/2003	2:36:27 PM	Service Control Manager	No
Information	1/22/2003	2:36:11 PM	Tcpip	No
Information	1/22/2003	4:32:29 AM	Service Control Manager	No
Information	1/22/2003	4:32:28 AM	Removable Storage Se...	No
Error	1/22/2003	4:07:11 AM	W32Time	No
Information	1/22/2003	4:06:51 AM	Browser	No
Error	1/22/2003	4:06:49 AM	Dhcp	No
Warning	1/22/2003	4:06:49 AM	Dhcp	No

Three classes of events tracked by Windows

Icon indicates event type

Events recorded in the System log

FIGURE P-3: Viewing event details



Date: 1/22/2003 Source: W32Time
Time: 4:07:11 AM Category: None
Type: Error Event ID: 34
User: N/A
Computer: LAPTOP

Description:

The time service has detected that the system time needs to be changed by -31535988 seconds. The time service will not change the system time by more than -54000 seconds. Verify that your time and time zone are correct, and that the time source time.windows.com (ntp.m|0x1|192.168.1.101:123->207.46.226.34:123) is working properly.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

Information from the System log

Additional details about the event

Click button to view the previous event

Click button to view the next event in the log

Click button to copy the description of the event to the Clipboard

TABLE P-2: Event Viewer columns

column	description
Type	Identifies the nature of the event, such as informational, a warning, or an error
Date and **Time**	Point when an event occurred, based on the computer's clock
Source	The object, such as the program, computer, or user, that logged the event
Category	Event classification if applicable, such as Logon/Logoff
Event	Number that identifies the specific event type; this number helps technical support personnel track events in the system
User	User associated with the event if applicable; the user is not responsible for most events, so the User entry is often N/A
Computer	Name of the computer where the event occurred

Managing an Event Log

Event logs grow in size as you work on your computer, but Event Viewer provides tools that help you view just the information you need and store the information you want to save for later. For example, you can apply a **filter** that allows you to view only events matching specified criteria, such as all events associated with a certain user. You can also search for a specific event using similar criteria. You probably don't want your active log to include events that happened long ago. With Event Viewer, you can **archive**, or save, your log periodically and then clear the archived events. Most administrators archive event logs on a regular schedule. Margaret wants John to explore filtering and locating events. John also wants to archive his System log and then clear the events to prevent the list from becoming too long. In this lesson, you will practice the first few steps of clearing a log, but you will not actually complete the procedure so as not to affect your system.

Steps 1 2 3 4

1. In the Event Viewer window, click **View** on the menu bar, then click **Filter**
   The System Properties dialog box opens with the Filter tab active, as shown in Figure P-4. You can deselect the Event types check boxes to view only events of a certain type or from a specified time period, or you can view events from a specified source, category, user, computer, or ID number.

QuickTip

To clear all the events in a log, right-click the appropriate log in the left pane (Application, Security, or System), then click Clear all Events.

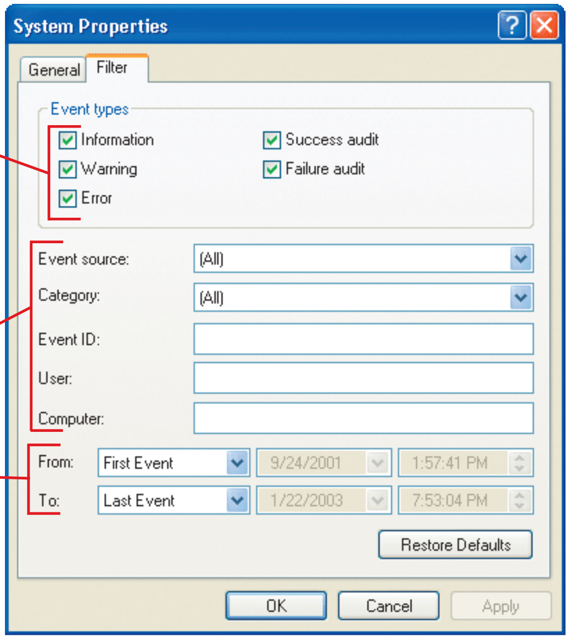
2. In the Event types section, deselect each check box except Error, then click **OK**
   The System Properties dialog box closes, and only error events appear in the System log. Depending on your computer system, you might not have any error events.
3. Click **View** on the menu bar, click **Filter**, click **Restore Defaults** in the System Properties dialog box, then click **OK**
   All events appear in the System log.
4. Click **View** on the menu bar, then click **Find**
   The Find in local System dialog box, shown in Figure P-5, allows you to search through all types of events or only certain types. You can specify a source, category, ID, computer, user, or description when searching for a particular event. Once you've specified what you are looking for, you click the Find Next button.
5. Click **Close**
   The Find in local System dialog box closes.
6. Right-click **System** in the left pane, then click **Save Log File As**
   The Save "System" As dialog box opens.

QuickTip

You can open the log you archived by using the Open Log File command on the Action menu in the Event Viewer window.

7. Click the **Save in list arrow**, navigate to the drive and folder where your Project Files are located, type **System** in the File name text box, then click **Save**
   You have saved the system event log in a file with an .evt extension.
8. Click the **Close button** in the Event Viewer window
   The Event Viewer window closes, and you return to the Administrative Tools window.

FIGURE P-4: Filtering an event log



System Properties

General | Filter

Event types

☑ Information ☑ Success audit
☑ Warning ☑ Failure audit
☑ Error

Event source: (All)
Category: (All)
Event ID:
User:
Computer:

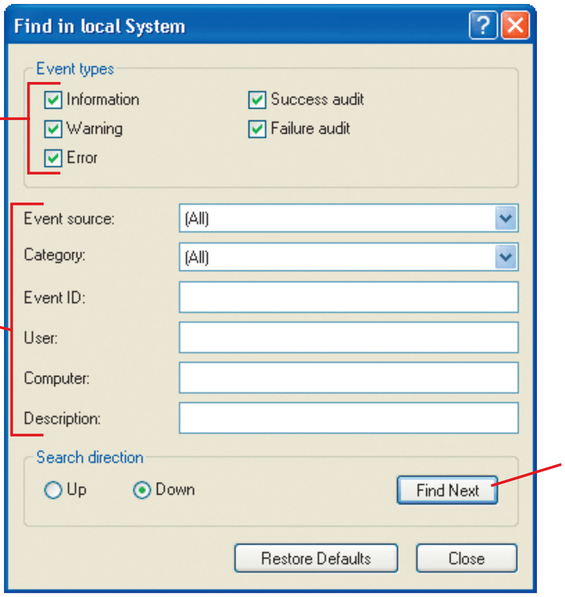
From: First Event 9/24/2001 1:57:41 PM
To: Last Event 1/22/2003 7:53:04 PM

Filter by event type

Filter by a specific value

Filter by date

FIGURE P-5: Find in local System dialog box



Find in local System

Event types

☑ Information ☑ Success audit
☑ Warning ☑ Failure audit
☑ Error

Event source: (All)
Category: (All)
Event ID:
User:
Computer:
Description:

Search direction

○ Up ● Down

Search for specific types of events

Search for a specific value

Click button to locate next event matching your criteria

Changing log settings

You can control how any log in the Event Viewer collects data by defining a maximum log size (the default is 512K) and instructing Event Viewer how to handle an event log that has reached its maximum size. Only users with administrative rights can change log settings. When the log—Application, Security, or System—is selected in the left pane of the Event Viewer window, you can click the Properties button on the toolbar to open the Properties dialog box, which allows you to change log settings. In addition to specifying a maximum log size, you can also choose from three log options when the log is full: new events can automatically overwrite the oldest events, new events can overwrite only events older than a specified number of days, or you can set Event Viewer not to overwrite events, in which case you must manually clear a full log before it can resume logging events.

Creating a Performance Chart

On a daily basis, your system generates a variety of performance data, such as your computer's memory or processor use, or the amount of congestion on a device. As the system administrator, you can use the Performance tool to create charts from the data that enable you to observe how a computer's processes behave over time. The types of performance data you monitor and record are called **performance objects**. Each performance object has a set of **counters** associated with it that provide numeric information. The Performance tool charts the numeric data gathered from the counters and provides graphical tools to make it easier to analyze and track the performance of your computer. Margaret helps John create a performance chart documenting the activities of the computer's processor.

Steps

QuickTip

If the default counters don't track the data you want, you can delete them and add the ones you want at any time.

1. In the Administrative Tools window, double-click the **Performance icon**, then click the **View Graph button** on the System Monitor toolbar in the Performance window if necessary

   The Performance window opens, as shown in Figure P-6, and begins charting the default counters listed at the bottom of the window. The right pane displays a chart of the object's performance. From the left pane you can create log files that record the performance values in text format.

2. Delete each counter by clicking the **Delete button** ✕ on the System Monitor toolbar, then click the **Add button** + on the System Monitor toolbar

   Your chart will be difficult to read if you do not limit the number of counters shown on the chart. The Add Counters dialog box opens, displaying a list of performance objects and their counters that you can select to chart as shown in Figure P-7. You want to chart one of the counters associated with the computer's processor.

3. Click the **Performance object list arrow**, then click **Processor** if necessary

QuickTip

To see what a counter measures, click the counter in the Counter list, then click Explain.

4. Click **%Privileged Time** in the Select counters from list, then click **Add**

   The %Privileged Time counter monitors the percentage of the time the processor spends working with hardware, system memory, and other **privileged system components**, which are Windows operating system processes or tasks in progress. The Performance tool immediately begins charting this counter, though you may not be able to see the chart if the Add Counters dialog box obscures it on your screen.

QuickTip

To show accurate processor use in a performance chart, disable screen savers in the Control Panel, as they take up processor resources and give your chart a distorted view of processor performance.

5. Click **%Processor Time** in the Select counters from list, then click **Add**

   This counter measures the percentage of time that the processor is busy executing commands, known as a **non-idle thread**; it is a primary indicator of processor activity.

6. Click **%User Time**, then click **Add**

   The %User Time counter measures time spent on requests from user applications.

7. Click **Close** in the Add Counters dialog box

   A red bar moves across the screen, and the chart shows the performance of the three counters as colored lines on the chart.

QuickTip

To highlight a line, click the counter object at the bottom of the chart, then click the Highlight button on the System Monitor toolbar.

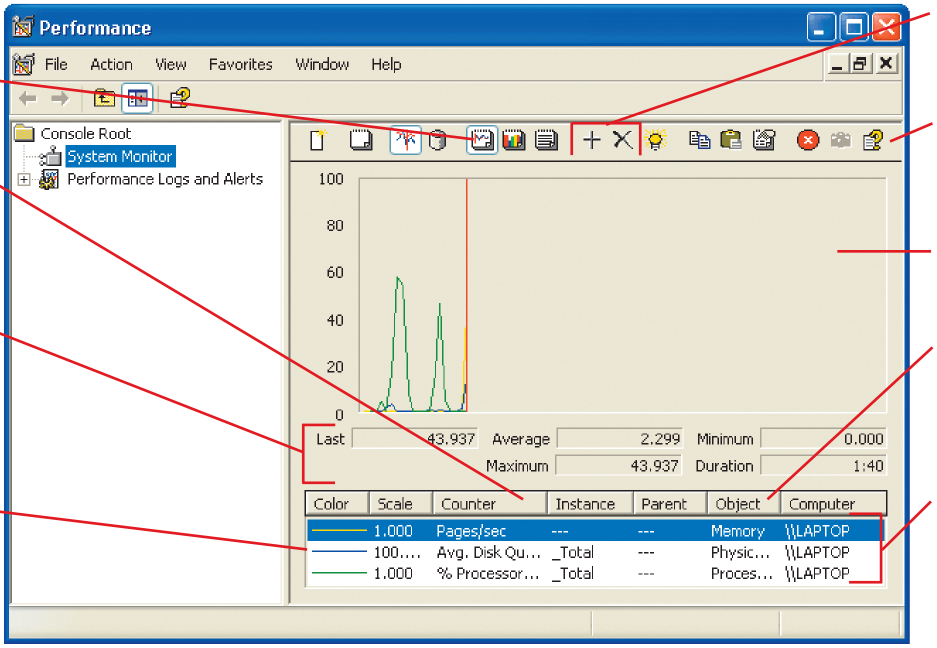
8. Double-click the time in the notification area of the task bar, click **Cancel** in the Date and Time Properties dialog box, then click the **Start button** on the taskbar twice

   Watch how the measure of processor time jumps up when activity occurs.

9. Click the **Freeze Display button** on the System Monitor toolbar

   The performance counters stop tracking events.

FIGURE P-6: Charting system performance



Console Root
- System Monitor
- Performance Logs and Alerts

Last 43.937 Average 2.299 Minimum 0.000
Maximum 43.937 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
🟨	1.000	Pages/sec	---	---	Memory	\\LAPTOP
🟦	100....	Avg. Disk Qu...	_Total	---	Physic...	\\LAPTOP
🟩	1.000	% Processor...	_Total	---	Proces...	\\LAPTOP

View Graph button

Counter type

Statistics about the most recent reading for the selected counter

Color-coded lines distinguish each counter

Click buttons to add and delete counter objects

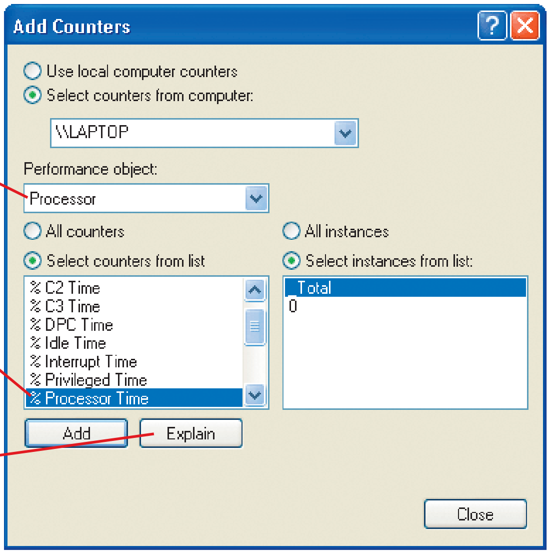
System Monitor toolbar

Your chart will differ

Performance object type

List of charted performance counters

FIGURE P-7: Selecting performance counters to chart



○ Use local computer counters
● Select counters from computer:

\\LAPTOP

Performance object:

Processor

○ All counters
● Select counters from list

% C2 Time
% C3 Time
% DPC Time
% Idle Time
% Interrupt Time
% Privileged Time
% Processor Time

○ All instances
● Select instances from list:

_Total
0

Type of performance object

Counter list; displays counters associated with the performance object

Click button to read an explanation of the selected counter

CLUES TO USE

Baseline charts

Performance charts include statistics about each counter you select, but unless you know how your system should perform, these statistics might not be very meaningful. For this reason, administrators create **baseline charts**, charts made when the computer or network is running at a normal level. When there are problems, the administrator can create another performance chart that can be compared to the baseline chart. By regularly creating and comparing performance charts, administrators can anticipate and then prevent problems.

Setting Up an Alert

In addition to creating performance charts, you can use the Performance window to create user alerts. An **alert** is a warning that is automatically generated when a counter value exceeds or falls short of a threshold value you have specified. When an alert condition is met, the date and time of the event are recorded in the Application log, which you can view from the Event Viewer. For example, you can set the %User Time alert to monitor the percentage of elapsed time the computer spends running programs. Some programs require more processing time than others, which can slow down your computer. The %User Time alert can let you know if your programs are using too many resources and slowing down your computer. Your system can record up to 1,000 alert events, after which the oldest events are discarded as new events occur. Margaret guides John through setting up an alert to monitor the use of the computer's processor. The alert will occur whenever the percentage of the time the processor is in use exceeds a certain threshold, such as 75%.

Steps 1 2 3 4

1. In the Performance window, click the **Performance Logs and Alerts icon** in the left pane, then double-click **Alerts** in the list that opens in the right pane
2. Click **Action** on the menu bar, then click **New Alert Settings**
   The New Alert Settings dialog box opens. Each alert requires a specific name, so you first have to give it a name to identify it to the performance monitor.
3. In the Name box, type **Alert Test**, then click **OK**
   The Alert Test dialog box opens. From this dialog box, you specify which counters you want to track, and under what conditions the alert will be triggered.
4. Click **Add**
   The Add Counters dialog box opens.
5. If necessary, click the **Performance object list arrow**, then click **Processor**
6. Click **%Processor Time** in the Select counters from list, click **Add**, then click **Close**
   The Add Counters dialog box closes, and the Alert Test dialog box appears.
7. Click the **Alert when the value is list arrow**, click **Over** if necessary, then type **75** in the Limit text box
   An alert will be added to the alert log when processor time exceeds 75%, as shown in Figure P-8
8. Click **OK**
   The Alert Test you just created appears in the right pane of the Performance window. The icon appears green when it is running and red when it is not.
9. Right-click the **Alert Test icon**, click **Delete**, click **OK** if the Performance Logs and Alerts message box opens, then click the **Close button** in the Performance window
   You return to the Administrative Tools window.

QuickTip

To monitor additional counters, repeat Steps 4-7 for each counter.

QuickTip

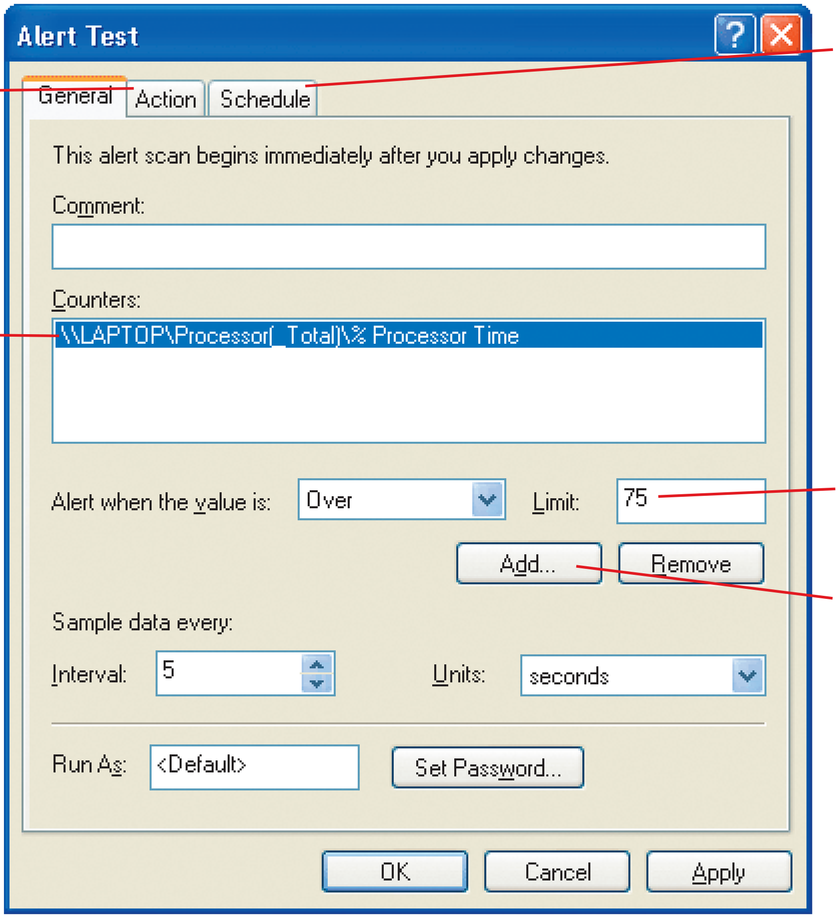
To stop an alert, select the alert in the right pane, then click the Stop the selected alert button ■ on the toolbar.

Clues to Use

Alert actions and schedules

The Action tab in the selected alert's Properties dialog box allows you to specify what action you want to take when your system triggers an alert. By default, the system logs an entry in the application event log when it triggers an alert. You can also specify that the system send a message to the network administrator, that performance data be collected, or that a specific program be run. To run a program, click the Browse button, specify the program path, then click OK. You can also schedule alerts using the Schedule tab in the selected alert's dialog box. Your system will scan for an alert at the times or intervals you specify.

FIGURE P-8: Creating a performance alert



This alert scan begins immediately after you apply changes.

Comment:

Counters: \\LAPTOP\Processor(_Total)\% Processor Time

Alert when the value is: Over

Limit: 75

Sample data every:

Interval: 5

Units: seconds

Run As: <Default>

Click the Action tab to choose an action when the alert condition is met

Your path will vary

Click the Schedule tab to schedule a time to automatically check for alerts

Threshold value

Click button to add additional counters

CLUES TO USE

Managing your computer's performance

You can adjust Windows XP to improve its performance by changing the way Windows XP manages system processing and memory. You can set Windows XP to give a greater proportion of processor time to the program in which you are currently working, known as a **foreground process**. The greater the processor time, the faster response time you receive from the program in which you are currently working. If you have **background processes**, such as printing, that you want to run while you work, you might want to have Windows XP share processor time equally between background and foreground programs. To optimize performance for foreground and background processes, double-click the System icon in the Control Panel, click the Advanced tab in the System Properties dialog box, click Settings in the Performance section, click the Advanced tab, then click the Programs option button if necessary to optimize for foreground processes, or click the Background services option button to optimize for background processes. When your computer is running low on RAM and more is needed immediately to complete your current task, Windows XP uses hard disk drive space to simulate system RAM. This is known as **virtual memory**. For processes that require a lot of RAM, you can optimize virtual memory use by allocating more available space on your hard disk drive. In the Virtual memory section, click Change, then enter the initial size and maximum size you want to allocate for virtual memory use.

Viewing Computer Management Tools

Computer Management consolidates administrative tools, including those you've already used, such as Event Viewer and Performance, into a single window that you can use to manage a local or remote computer. When you open Computer Management, the Computer Management window uses a two-pane view that is similar to Windows Explorer. The hierarchy of tools in the left pane of the Computer Management window is called a **console tree**, and each main category of tools is called a **node**. The three nodes in the Computer Management window (System Tools, Storage, and Services and Applications), allow you to manage and monitor system events and performance and to perform disk-related tasks. Each node contains **snap-in tools**, which come in two types: standalone or extension. Standalone snap-ins are independent tools, while extension snap-ins are add-ons to current snap-ins. To perform an administrative task, you might need to navigate the hierarchy before you select a tool in the console tree. The selected tool appears in the right pane, and you can use the toolbars and menus that appear to take appropriate action with the tool. Margaret asks John to practice using Computer Manager by viewing the Application log to see how his alert was monitored.

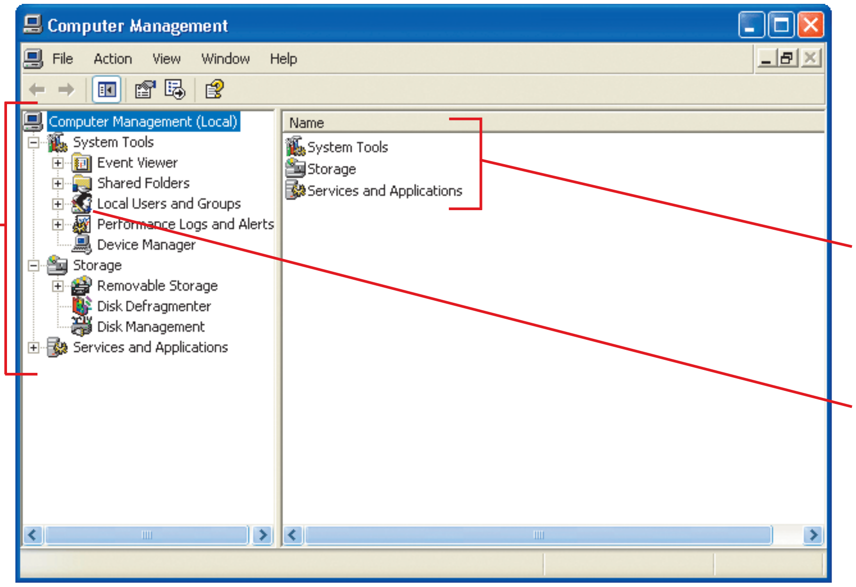
Steps

1. In the Administrative Tools window, double-click the **Computer Management icon**
   The Computer Management window opens, displaying two panes, as shown in Figure P-9. The left pane lists the hierarchy of tools; you navigate the tools using Expand indicators ⊞ and Collapse indicators ⊟ to display and hide objects in the tool hierarchy.
2. Click **System Tools** in the console tree (the left pane)
   The snap-in tools associated with System Tools appear in the right pane. The detailed list displays the snap-in tool type and a description.
3. Click the **Expand indicator** ⊞ next to System Tools to view the tools in the System Tools node if necessary
4. Click ⊞ in the console tree next to Event Viewer to view the event logs if necessary
5. Click **Application** under the Event Viewer
   Application events appear in the right pane.
6. Double-click the first **Information event** in the Application log list.
   If you have been working through the lessons without pausing, the Application log should show two Information events related to the Alert Test event, as well as many others. Figure P-10 shows the first event; it notes that the conditions of the Alert Test have been met.
7. Click **Cancel** to close the Event Properties dialog box
   You return to the Computer Management window.
8. Click the **Collapse indicator** ⊟ in the console tree next to Event Viewer

QuickTip

Notice that the System Tools node lists the Performance Logs and Alerts tools a little further down, where you can make changes to current logs and alerts.

FIGURE P-9: Computer Management window

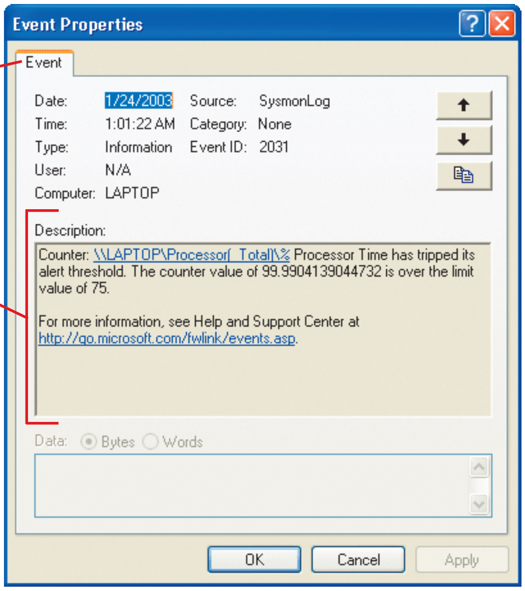


Windows administrative tools organized into one list

Nodes

Available only in the Professional edition

FIGURE P-10: Viewing an alert event



Date: 1/24/2003 Source: SysmonLog
Time: 1:01:22 AM Category: None
Type: Information Event ID: 2031
User: N/A
Computer: LAPTOP

Description:

Counter: \\LAPTOP\Processor(_Total)\% Processor Time has tripped its alert threshold. The counter value of 99.9904139044732 is over the limit value of 75.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

Your event will differ

Description of the event indicates that the alert conditions have been met

CLUES TO USE

Understanding local users and groups

In Windows XP Professional, you can manage the access privileges and permissions of local user and group accounts. A local user account is an individual account with a unique set of permissions, while a group account is a collection of individual accounts with the same set of permissions. You can change local user and group accounts in the Computer Management window using the Local Users and Groups tool. This security feature limits individual users and groups from accessing and deleting files, using programs such as Backup, or making accidental or intentional system-wide changes. You can create or modify a user account, disable or activate a user account, identify members of groups, and add or delete members to and from groups. To perform these account tasks and many others, click the Expand indicator ⊞ next to Local Users and Groups in the Computer Management window, click the Users or Groups folder icon below it, then double-click an account icon or select a command on the Action menu.

Understanding Disk File Systems

A disk must be formatted with a **file system** that allows it to work with the operating system to store, manage, and access data. Two of the most common file systems are FAT (or FAT32, which is an improvement on FAT technology) and NTFS. Disks on DOS, Windows 3.1, or Windows 98 computers use the FAT file system, while disks on computers running Windows NT 4.0 and later (including Windows XP) can use either the NTFS or FAT system. NTFS is a newer file system that improves on some of the shortcomings of FAT disks that make them less desirable on a network. Table P-3 describes the improvements of the NTFS file system over the FAT file system. Which file system your disks are most likely to use and why depends on the type of disk, whether your computer is on a network, and your computer's role as a resource on the network. Margaret explains the features of file systems to John.

Details

There are important differences between FAT and NTFS file systems:

FAT

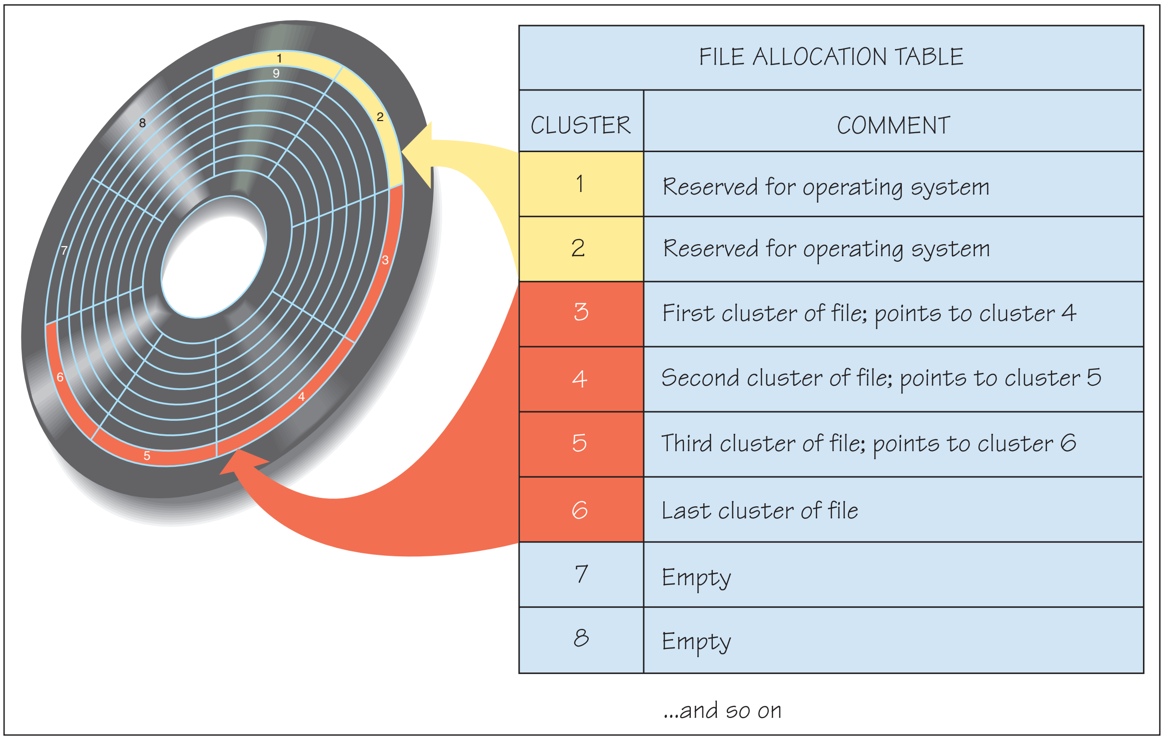
When you format a disk with the FAT file system, a formatting program divides the disk into storage compartments. First it creates a series of rings, called **tracks**, around the circumference of the disk. Then it divides the tracks into equal parts, like pieces of a pie, to form sectors, as shown in Figure P-11. The number of sectors and tracks depends on the size of the disk.

Although the physical surface of a disk is made of tracks and sectors, a file is stored in clusters. A cluster, also called an **allocation unit**, is one or more sectors of storage space. It represents the minimum amount of space that an operating system reserves when saving the contents of a file to a disk. Thus, a file might be stored in more than one cluster. Each cluster is identified by a unique number. The first two clusters, shown in yellow in Figure P-11, are reserved by the operating system. The operating system maintains a file allocation table (or FAT) on each disk that lists the clusters on the disk and records the status of each cluster: whether it is occupied (and by which file), available, or defective. Each cluster in a file "remembers" its order in the chain of clusters—and each cluster points to the next one until the last cluster, which marks the end of the file.

NTFS

NTFS features a built-in security system that does not allow users to access the disk unless they have a user account and password with the necessary rights and permissions. NTFS protects disks from damage by automatically redirecting data from a bad sector to a good sector without requiring you to run a disk-checking utility. Given the reliability and the built-in repair mechanisms of NTFS disks, only rarely do they require maintenance. This is an example of **fault tolerance**, the ability of a disk to resist damage, which is a critical issue with disks on a network computer.

FIGURE P-11: Files stored in clusters



FILE ALLOCATION TABLE	
CLUSTER	COMMENT
1	Reserved for operating system
2	Reserved for operating system
3	First cluster of file; points to cluster 4
4	Second cluster of file; points to cluster 5
5	Third cluster of file; points to cluster 6
6	Last cluster of file
7	Empty
8	Empty

...and so on

TABLE P-3: NTFS improvements on the FAT file system

feature	FAT	NTFS
Security	Vulnerable to "hackers"—unauthorized users who break into other people's files	Includes built-in security measures that allow only people who have permission to access files
Recoverability	Likely to fail if a sector containing system data is lost because they store critical system files in single sectors	Highly reliable because it uses redundant storage—it stores everything in vital sectors twice, so if a disk error in a vital sector occurs, NTFS can access file system data from the redundant sector
File size	Designed for small disks (originally less than 1 MB in size); can handle a maximum file size of 4 GB	Handles files up to 64 GB in size

CLUES TO USE

Selecting a file system

NTFS does not support floppy disks, so all floppies are formatted with FAT. If you are running Windows XP on a stand-alone computer, you can choose either FAT or NTFS, but in most cases, the file system has already been determined either by the person who originally set up the computer or by the manufacturer from whom you purchased the computer. If your computer is a client on a Windows XP network, it is likely that your hard disk uses NTFS. Because NTFS is more suited to network demands, such as a high level of security and resistance to system failure, network administrators format network disks with NTFS whenever possible. Sometimes, however, users on a network want or need to use a non-Windows XP operating system. Also, a user might need a computer that is capable of running Windows XP or Windows 98/Me. The disks on that computer would then be formatted with FAT.

Managing Disks

The Storage node in the Computer Management window provides you with tools, such as Disk Defragmenter and Disk Management, to help you manage your disks. The Disk Management tool is a graphical tool for managing disks that allows you to partition unallocated portions of your disks into volumes. A **volume** is a fixed amount of storage on a disk. A single disk can contain more than one volume, or a volume can span part of one or more disks. Each volume on a disk is assigned its own drive letter, which is why the term volume is often synonymous with the term drive. Thus, the same physical disk might contain two volumes. Each volume can use a different file system, so you might have a single disk partitioned into two volumes, each with its own file system. Figure P-12 shows how you might partition a single hard disk in two different ways: first, with a single NTFS volume, and second, with one NTFS volume and one FAT volume, which can be helpful if you have a computer with two operating systems, Windows 98 on the FAT volume and Windows XP on the NTFS volume. Margaret suggests that John view the storage tools.

Steps 1 2 3 4

1. In the Computer Management window, click the **Expand indicator** ⊞ next to the Storage node if necessary
2. In the console tree, click **Disk Management**
   The disks on your computer appear in the right pane. The top right pane of the window displays your computer's volumes, and the bottom right pane offers a graphic display of the breakdown of space on each disk, allowing you to see how your disks are partitioned. Figure P-13 displays a computer with a hard disk and a CD-ROM disk, assigned to drive letter D. The hard disk, labeled Disk 0, has only one FAT drive, assigned to drive letter C:, and no unallocated space. The 0 in the label Disk 0 indicates the disk number, starting from 0, for each disk type disk on the computer. Hard and removable disks are one disk type, while CD-ROMs and DVDs are another.
3. Click the **Settings button** on the toolbar
   The Settings dialog box opens, as shown in Figure P-14, allowing you to change the color or pattern of any disk region displayed in the Disk Management window. Refer to the Disk region list in Figure P-14 to identify the disk regions that you might see on your drives. System administrators use many of the items in this list to create drives that are extremely reliable for data storage.
4. Click **Cancel** to close the Settings dialog box
5. In the console tree, click **Disk Defragmenter**
   The Disk Defragmenter program window appears in the right pane. You can analyze and defragment a disk from the Computer Management window.
6. Click the **Close button** in the Computer Management window

CLUES TO USE

Partitioning a disk

If you have a computer at home, its disks are most likely already partitioned, and partitioning those disks further can be laborious if there is no available **free space** (space that is not yet part of a partition). If, however, you have the necessary rights on a computer whose disk or disks have available unallocated space, you can partition your disk. You right-click an unallocated region of a disk in the Disk Management pane, then click Create Partition. You then follow the Create Partition Wizard directions that appear on your screen. This wizard helps you format your new drive, so you can store data on it.

FIGURE P-12: A hard disk, partitioned two different ways

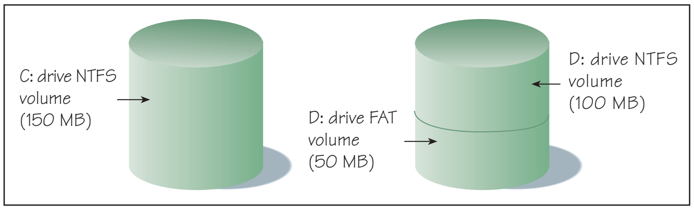
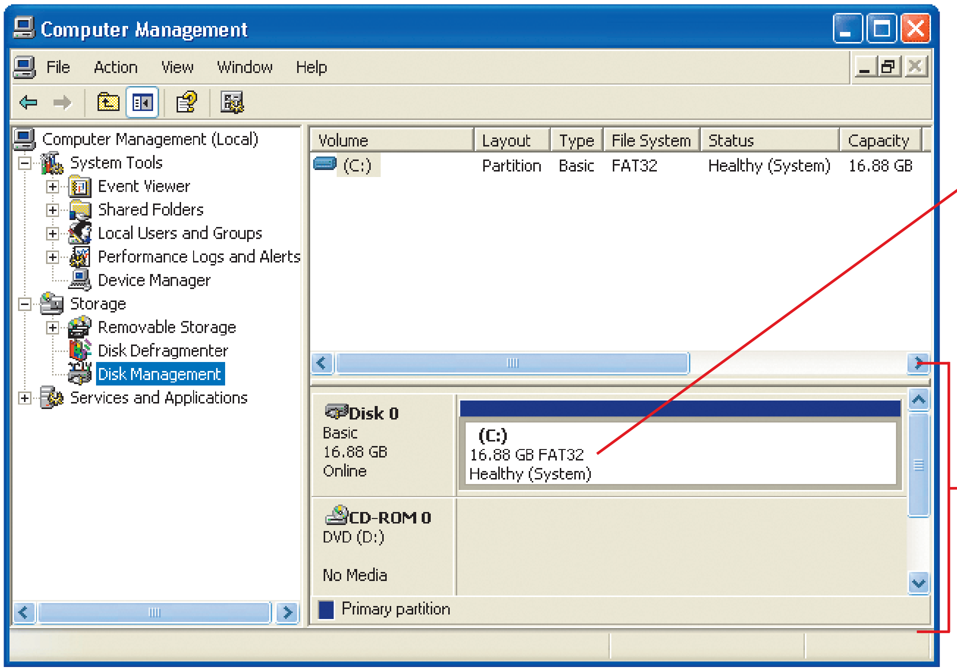

C: drive NTFS volume (150 MB)
D: drive FAT volume (50 MB)
D: drive NTFS volume (100 MB)

FIGURE P-13: Viewing Disk Management information



Computer Management (Local)
- System Tools
  - Event Viewer
  - Shared Folders
  - Local Users and Groups
  - Performance Logs and Alerts
  - Device Manager
- Storage
  - Removable Storage
  - Disk Defragmenter
  - Disk Management
- Services and Applications

Volume	Layout	Type	File System	Status	Capacity
(C:)	Partition	Basic	FAT32	Healthy (System)	16.88 GB

Disk 0
Basic
16.88 GB
Online

(C:)
16.88 GB FAT32
Healthy (System)

CD-ROM 0
DVD (D:)

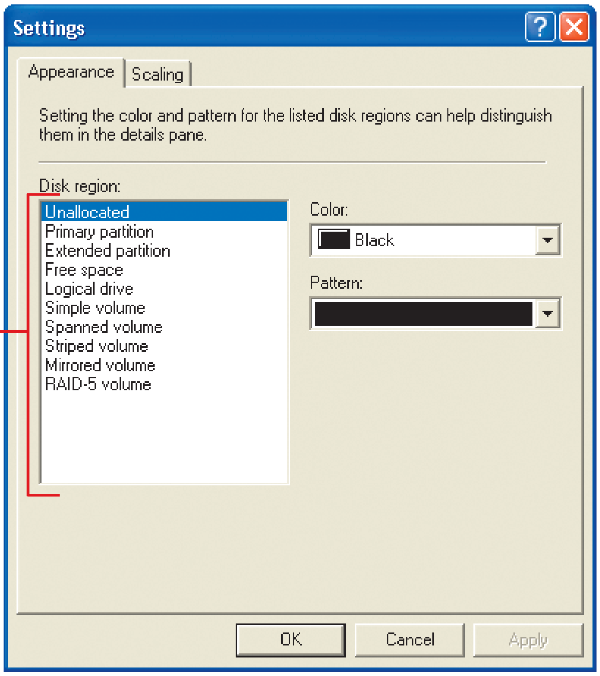
No Media

■ Primary partition

Drive is formatted using the FAT32 file system

Two drives on the system

FIGURE P-14: Settings dialog box



Setting the color and pattern for the listed disk regions can help distinguish them in the details pane.

Disk region:
- Unallocated
- Primary partition
- Extended partition
- Free space
- Logical drive
- Simple volume
- Spanned volume
- Striped volume
- Mirrored volume
- RAID-5 volume

Color: ■ Black

Pattern:

These items can be displayed in the Computer Management window

Monitoring Local Security Settings

Using Windows XP Professional, you can view and monitor local security settings with the Local Security Settings tool to ensure that computer users are adhering to the organization's security policies. For example, you can set user account and password options to require computer users to create complex passwords of a specific length and change them on a regular basis. A **complex password** contains characters from at least three of the four following categories: uppercase (A through Z), lowercase (a through z), numbers (0 through 9), and nonalphanumeric (!, $, *, etc.). In addition to setting security options, you can also **monitor**, or **audit**, the success or failure of security related events, such as account logon and logoff activities, user account changes, and program launches. When an event that you have chosen to audit is triggered, it appears in the Event Viewer in the Security node. Margaret suggests that John learn how to view and monitor local security settings.

Steps

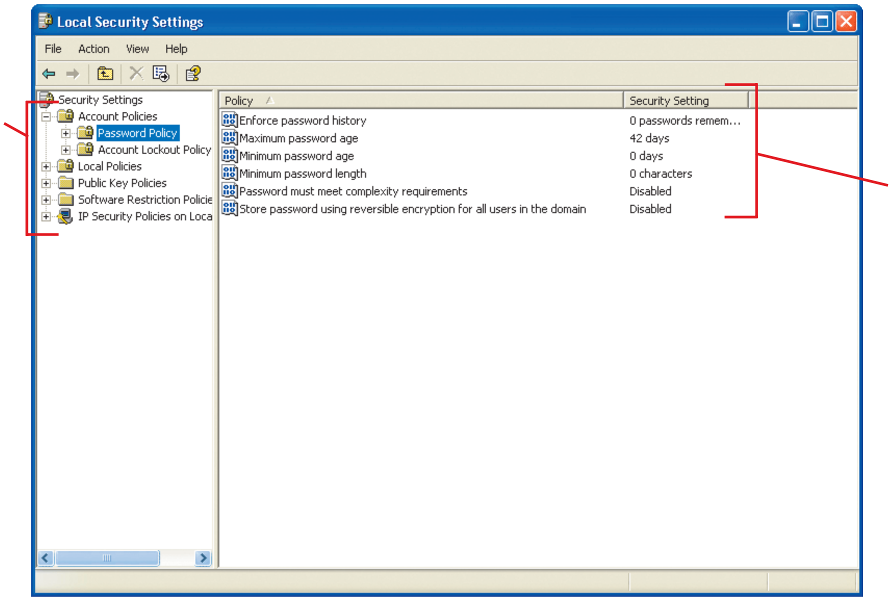
If you are using Windows XP Home edition, you will not be able to work through the steps in this topic. Read the topic without completing the steps.

1. In the Administrative Tools window, double-click the **Local Security Policy icon**
   The Local Security Settings window opens, with a two-pane view like Windows Explorer.
2. Click the **Expand indicator** ⊞ next to Account Policies, then click the **Password Policy folder**
   Password Policy displays current password policies and settings, as shown in Figure P-15.
3. In the right pane, double-click **Maximum password age**, then click **Cancel** to avoid making any changes
   The Maximum password age Properties dialog box displays a numeric box in which you can change the number of days until a password expires.
4. Click ⊞ next to Local Policies, then click the **Audit Policy folder**
   Audit Policy displays security events you can monitor in the Event Viewer.
5. In the right pane, double-click **Audit account logon events** to open its Properties dialog box, click the **Success check box** to select it, then click **OK**
   Audit account logon events policy changes to "Success," as shown in Figure P-16.
6. Click the **Start button** on the taskbar, click **Log Off**, click **Switch User**, then log on again with your account or the administrator account
   Logging off and on your computer triggers the local security policy event.
7. In the Local Security Settings window with Audit Policy selected, double-click **Audit account logon events** in the right pane to open its Properties dialog box, click the **Success check box** to deselect it, click **OK**, then click the **Close button** in the Local Security Settings window
   The audit policy is restored to its original settings, and the Local Security Settings window closes.
8. In the Administration Tools window, double-click the **Event Viewer icon** to open the Event Viewer window, then click **Security** in the left pane
   The successful audit events appear in the Event Viewer, as shown in Figure P-17.
9. Scroll to the right and change column widths if necessary to display audit information, then click the **Close** button in the Event Viewer, Administrative Tools, and Control Panel windows

Trouble?

If Switch User is not available, click Logoff, close all programs if necessary, log on again, then open the Administration Tools window via the Control Panel and start Local Security Settings.

FIGURE P-15: Password policies with current settings



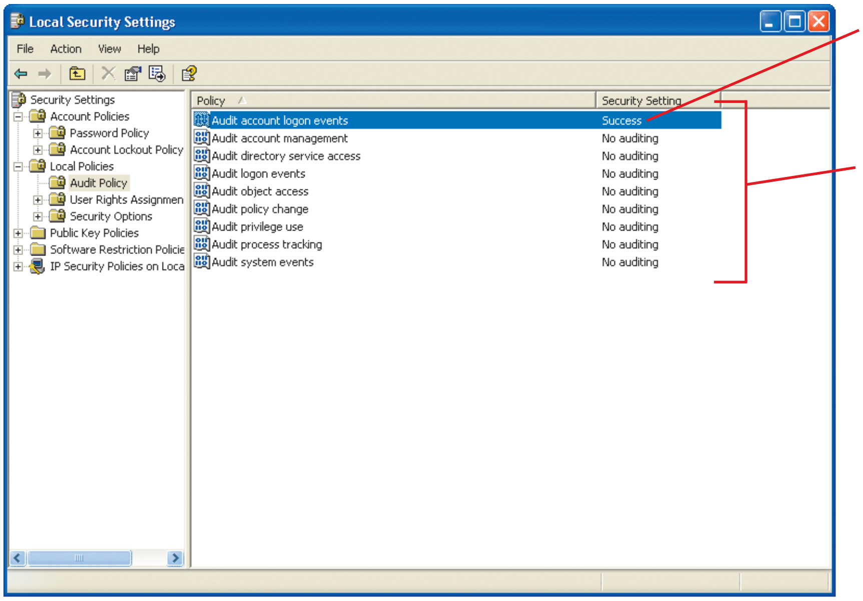
Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
- Public Key Policies
- Software Restriction Policie
- IP Security Policies on Loca

Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled

Security Settings categories

Password policies you can change

FIGURE P-16: Audit policies with current settings



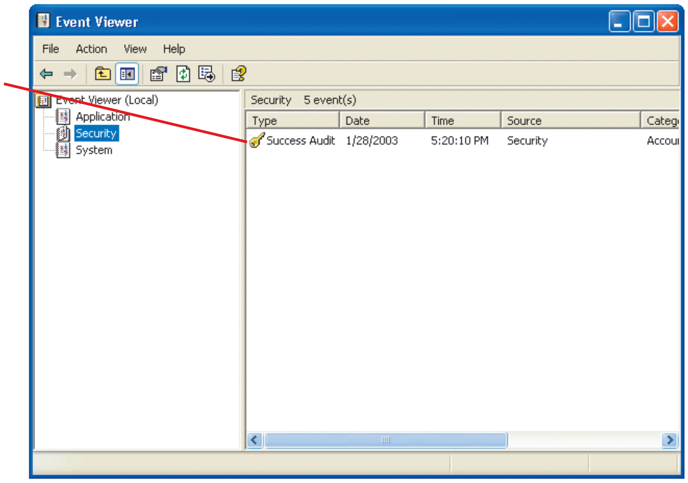
Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
  - Audit Policy
  - User Rights Assignmen
  - Security Options
- Public Key Policies
- Software Restriction Policie
- IP Security Policies on Loca

Policy	Security Setting
Audit account logon events	Success
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit policy activated for successful events

Audit policies you can monitor

FIGURE P-17: Event Viewer window with successful audit event



Event Viewer (Local)
- Application
- Security
- System

Security 5 event(s)

Type	Date	Time	Source	Categ
Success Audit	1/28/2003	5:20:10 PM	Security	Accou

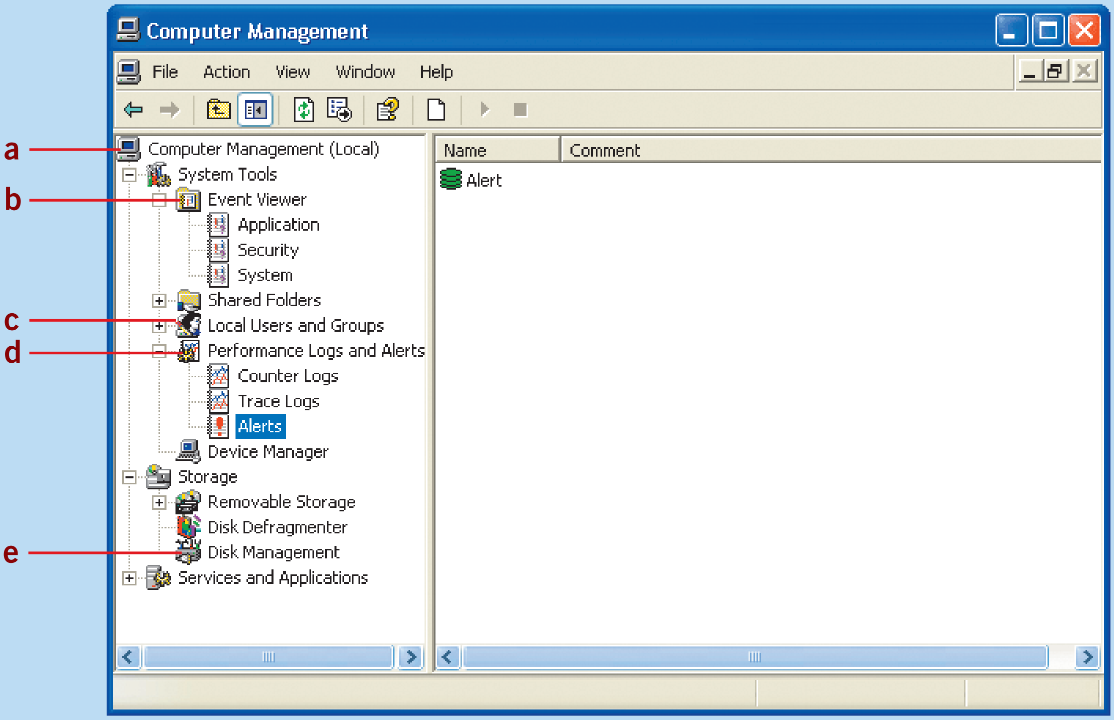
Successful audit event; your list might differ

Practice

Concepts Review

Label each element of the screen shown in Figure P-18.

FIGURE P-18



1. Which element points to the tool that displays monitoring and troubleshooting messages from the system and other programs?
2. Which element points to the tool that displays graphs of system processes and configures data logs and alerts?
3. Which element points to the tool that provides access to administrative tools to manage local and remote computers?
4. Which element points to the tool that limits users from accessing and deleting files, using programs, or making system-wide changes?
5. Which element points to the tool that manages volumes and creates partitions?

Match each of the terms with the statement that describes its function.

6. Performance Monitor	a. Allows you to examine System, Security, and Application logs
7. NTFS	b. Allows you to log an alert
8. Disk Management	c. Uses redundant storage
9. Volume	d. Allows you to create a partition
10. Counter	e. When a computer or network is running at a normal level
11. FAT	f. Storage space that can span one or more disks
12. Baseline	g. Designed for small disks
13. Event Viewer	h. Numerical information about the performance of an item on your computer

Practice

Select the best answer from the list of choices.

14. The Computer Management window contains tools that allow you to:
- **a.** Install new programs.
- **b.** Change your display settings.
- **c.** View but not change system information.
- **d.** Track performance data.

15. If you want your computer to create an alert when your processor is running at 85%, which tool should you use?
- **a.** Disk Administrator
- **b.** Event Viewer
- **c.** Performance Monitor
- **d.** User Manager

16. If an alert threshold value is reached, Windows will:
- **a.** Add an alert event to the Event Log.
- **b.** Send e-mail to the network administrator.
- **c.** Shut down the computer.
- **d.** Print a diagnostic report.

17. To interpret a performance chart, an administrator should compare it to:
- **a.** A Windows diagnostic report.
- **b.** The Event Viewer System log.
- **c.** A list of volumes in Disk Management.
- **d.** A baseline chart.

18. What is a counter?
- **a.** An object such as a processor or physical disk
- **b.** A program you can run when an alert reaches a threshold value
- **c.** A numeric value that measures the performance of an object
- **d.** A red bar on the Performance Monitor chart that indicates an object's status

19. FAT stands for:
- **a.** File allocation track.
- **b.** Format allocation track.
- **c.** File allocation table.
- **d.** Format allocation table.

20. The Disk Management tool allows you to partition disks into:
- **a.** Clusters.
- **b.** Volumes.
- **c.** Sectors.
- **d.** Tracks.

► Skills Review

1. Explore Windows administrative tools.
- **a.** Open the Control Panel, then double-click the Administrative Tools icon.
- **b.** Write down a sentence that describes each administrative tool.

2. Monitor activity with Event Viewer.
- **a.** Start Event Viewer, then click the Application icon in the left pane. If this log is empty, use another log, such as System.
- **b.** Double-click one of the entries to view a description of that event in the Event Properties window, click the up arrow or down arrow button to display other events, then click OK.

3. Manage an event log.
- **a.** In the Event Viewer window, click View on the menu bar, then click Filter.
- **b.** Deselect all the Event types check boxes except for Warning and Error, then click OK.
- **c.** View details on two of the events.
- **d.** Click View on the menu bar, click Filter, click Restore Defaults, then click OK.
- **e.** Click View on the menu bar, then click Find.
- **f.** Click the Event source list arrow, then click one of the programs in the list.
- **g.** Click Find Next. (The first event matching your criteria is selected in the event log; if you don't get a match, skip to Step i.)
- **h.** Double-click the event you just found, then click Cancel in the Event Properties window.
- **i.** Save the Application log as **Application** to the drive and folder where your Project Files are located, then close Event Viewer.

4. **Create a performance chart.**
   - **a.** Start Performance, then click the View Graph button on the System Monitor toolbar if necessary.
   - **b.** Click the Add button on the System Monitor toolbar, click the Performance object list arrow, then click Memory.
   - **c.** Add the Available Bytes, and the Committed Bytes counters, then click Close.
   - **d.** Allow the chart to generate for a few minutes, then identify which is greater, the number of available bytes or the number of committed bytes.
5. **Set up an alert.**
   - **a.** Click the Expand indicator next to Performance Logs and Alerts in the left pane, then click the Alerts icon.
   - **b.** Click Action on the menu bar, then click New Alert Settings.
   - **c.** Type **Alert Check**, then click OK.
   - **d.** Click Add, then select Processor in the Performance object list if necessary.
   - **e.** Click %Processor Time in the Counter list, click Add, then click Close.
   - **f.** Set the Alert when the value is option to Over, type 85 in the Limit text box, then click OK.
   - **g.** Return to the Performance window and delete the alert you just created.
   - **h.** Close Performance.
6. **View Computer Management tools.**
   - **a.** Start Computer Management, then open the Event Viewer folder.
   - **b.** Double-click Application in the right pane, double-click an event, then click OK.
   - **c.** Open Device Manager, then open Disk Defragmenter.
7. **Manage disks.**
   - **a.** In the Computer Management window, open Disk Management.
   - **b.** Identify the number of FAT volumes you have and the number of NTFS volumes if any.
   - **c.** Determine how physical disk space is used on your computer.
   - **d.** Write down two reasons why your computer's disks might be configured the way they are (consider the advantages of NTFS over FAT in a network environment).
   - **e.** Close Computer Management.
8. **View and save system information.**
   - **a.** Start Local Security Settings. If you are using Windows XP Home edition, skip these steps.
   - **b.** Open the Account Policies folder, then open the Password Policy folder.
   - **c.** Double-click a policy to view its options, then click Cancel.
   - **d.** Open the Local Polices folder, then open the Audit Policy folder.
   - **e.** Open the Audit policy change policy, select the Success check box, then click OK.
   - **f.** Open the Audit account management policy, select the Success check box, then click OK.
   - **g.** Open each policy you just changed and deselect the Success check box, then click OK to restore settings.
   - **h.** Close Local Security Settings.
   - **i.** Start Event Viewer, click the Security icon in the left pane to view the Policy Change triggered events, then close Event Viewer, the Administrative Tools window and the Control Panel window.

► Independent Challenge 1

You own a small bakery, and you just purchased a computer with Windows XP to help manage inventory, payroll, and other accounting procedures. You decide to create a baseline chart using Performance that indicates how the computer performs in normal circumstances so you can monitor your system performance.

- **a.** Use Performance to create a chart with two Memory counters: %Committed Bytes In Use and Cache Bytes.
- **b.** Print the chart and put your name on the printout. (Press [Print Screen] to make a copy of the screen, open Paint, click Edit on the menu bar, click Paste to paste the screen into Paint, then click Yes to paste the large image if necessary. Click the Text button on the Toolbox, click a blank area in the Paint work area, then type your name.

Click File on the menu bar, click Page Setup, change 100% normal size to 50% in the Scaling area, then click OK. Click File on the menu bar, click Print, then click Print.)

c. Use the Explain button in the Add Counters dialog box to learn more about the two counters you charted. On the back of your printout, write a short description of both counters.

d. Close Performance.

► Independent Challenge 2

You own a small résumé preparation business. You are considering buying a new hard disk for your Windows XP computer, which you use to produce and store clients' resumes. Before you shop, you want to produce documentation on your current disk setup so that you can take your findings to different computer vendors and provide the sales representatives with the information they need to advise you. You use both Disk Management and Event Viewer.

a. Open the Computer Management window, then open the Disk Management folder.

b. Create a printout of your disk configuration and put your name on the printout. (See Independent Challenge 1, Step b for print screen printing instructions.)

c. Open the Event Viewer folder and use the Find feature to view all events related with "disk."

d. Open the disk event, then create a printout of Event Properties dialog box. (See Independent Challenge 1, Step b for print screen printing instructions.)

e. Close Computer Management.

► Independent Challenge 3

You are the systems administrator for the research and development (R&D) department at Herrera Pharmaceuticals. One of the R&D specialists has been having problems with her computer. You decide to start by examining the event logs, particularly the System log. You also want to check the log settings to make sure the log is collecting data properly.

a. Start Event Viewer, open the System log, then use the Filter feature to view only Error and Warning events.

b. Print the list and put your name on the printout. (See Independent Challenge 1, Step b for print screen printing instructions.)

c. Check Event Viewer settings using the Properties command on the Action menu. On the printout, write a summary of the current settings.

d. Save the System log as **Latest System** to the drive and folder where your Project Files are located.

e. Restore the default Filter settings, then close Event Viewer.

► Independent Challenge 4

You and some fellow students at your university have joined forces with a supplier of sweaters, blankets, and other handmade wares from Peru to create an international import business. You've been using an older computer with Windows XP, and you are concerned because your computer runs rather slowly. You decide to run some tests on the processor and memory and gather some information about how you might improve your computer's performance.

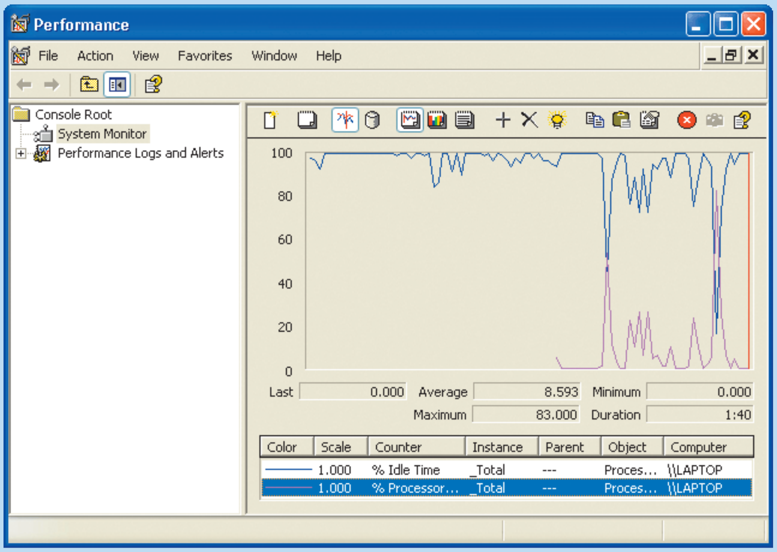
a. Use Performance to create two charts, one on memory and one on your computer's processor. Use three counters for each chart. Use the Explain button in the Add Counters dialog box to learn more about the counters.

b. Print the charts. (See Independent Challenge 1, Step b for print screen instructions.) On the back of each printout, describe the counters and explain the chart results, then close Performance.

► Visual Workshop

This exercise can be completed by users of both Windows XP Professional and Home. Re-create and print the screen shown in Figure P-19, which displays a Performance chart. Your chart numbers will differ. Print the screen. (See Independent Challenge 1, Step c for print screen printing instructions.)

FIGURE P-19

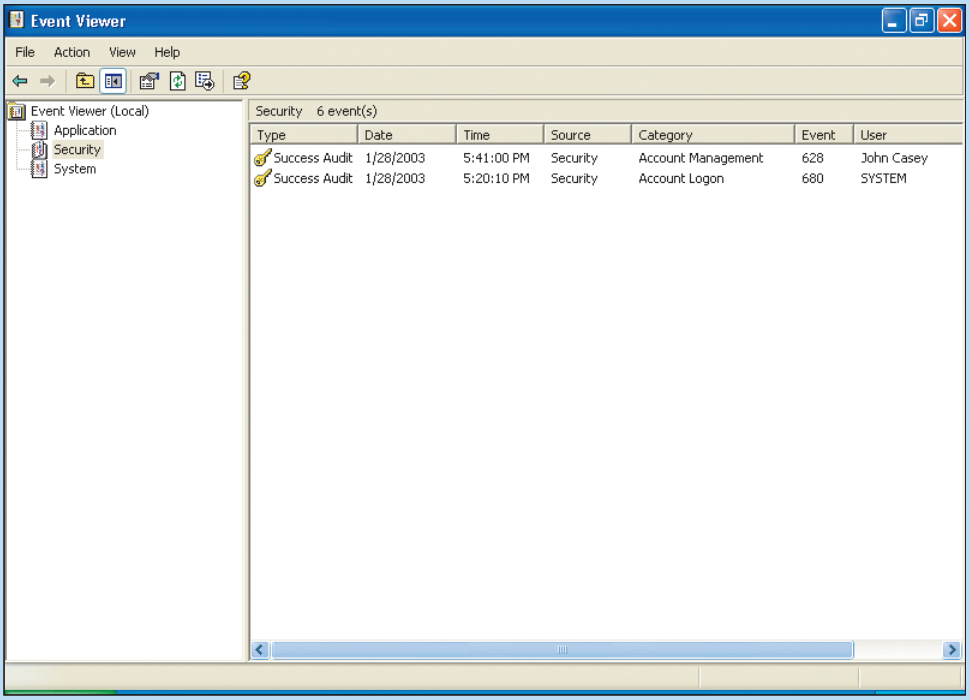


Last 0.000 Average 8.593 Minimum 0.000
Maximum 83.000 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
───	1.000	% Idle Time	_Total	---	Proces...	\\LAPTOP
───	1.000	% Processor...	_Total	---	Proces...	\\LAPTOP

This exercise can be completed only by users of Windows XP Professional. Re-create and print the screen shown in Figure P-20, which displays the Event Viewer window with the Security node selected in the left pane and audit events in the right pane. Your date, time, and user name will differ. Print the screen. (See Independent Challenge 1, Step c for print screen printing instructions.)

FIGURE P-20



Security 6 event(s)

Type	Date	Time	Source	Category	Event	User
Success Audit	1/28/2003	5:41:00 PM	Security	Account Management	628	John Casey
Success Audit	1/28/2003	5:20:10 PM	Security	Account Logon	680	SYSTEM